CROSSTALK
2000-03

OFFICE OF SECURITY AND EMERGENCY OPERATIONS

REPEATED COMPROMISES OF DOE WEB SERVERS USING KNOWN EXPLOITS

SUMMARY

There have been a series of defacements of DOE-owned World Wide Web servers that are running the Microsoft Internet Information Server (IIS) software. The known vulnerability in IIS has been well publicized in recent months in both the general press and on hacker bulletin boards. The exploit that takes advantage of this vulnerability is well known and easily available to anyone with Internet access. The patch to eliminate this vulnerability is also well-known, readily available, and takes less than 1 minute to implement on most machines– yet eleven DOE servers are known to have been compromised since October 15, 1999 using this exploit.

BACKGROUND

Hackers frequently probe public servers, checking for vulnerabilities that can be exploited. If a server is vulnerable, there is a high probability that it will be defaced. In one recent instance, a hacker successfully ran the exploit against a vulnerable DOE site, defacing the site's web page. The local system administrator took the system off-line, replaced the defaced page with the original page, and put the system back on-line – but without fixing the vulnerability. Within 4 hours, that machine was defaced again with the same exploit but by a different hacker. While this incident is anecdotal, it makes two points: (1) system administrators are not abiding by good security practices; and (2) vulnerable systems are easily detectable by a hacker. Hoping that your vulnerable system won't be discovered is not a winning strategy.

RECOMMENDATIONS

DOE's Computer Incident Advisory Capability (CIAC) issues Information Bulletins and Advisory Notices to all DOE sites when a system vulnerability is reported. Individuals responsible for Cyber Security throughout the Department, including system administrators, must evaluate the information provided in these bulletins and notices and determine if their systems are effected by the notification. Once the determination has been made that the specific bulletin or notice is applicable to their systems, these individuals are responsible for informing site management of the current risks associated with the vulnerabilities and the implications of not implementing corrective actions in a timely manner. If corrective measures cannot be implemented in a timely fashion, then it is the responsibility of these cyber security professionals to present senior site management with enough information to make an informed risk management decision.

Because of the relatively high number of web page defacements each site's senior management should take pro-active measures to ensure that the individuals responsible for web sites implement all of the relevant security patches to eliminate known vulnerabilities. CIAC Bulletin J-054, entitled "Unauthorized Access to IIS Servers through ODBC Data Access with RDS", contains the necessary information for system administrators to secure their IIS web servers. For further information regarding the IIS web server vulnerability, as well as vulnerability information for all types of information systems, please access the CIAC web page at: http://ciac.llnl.org/. Technical assistance can also be obtained by contacting the CIAC hotline on (925) 422-8193.